Jurnal Ilmiah Informatika
Volume 1 No. 1 / Desember 2016

IMPLEMENTASI ALGORITMA *ELGAMAL* DALAM SISTEM *LOCK* BRANKAS BERBASIS MIKROKONTROLER ATMEGA16 DAN *SMARTPHONE* ANDROID

Muhammad Rofiq [1)], Bambang Tri Wahjo Utomo [2)]
[1] Sistem Komputer, STMIK Asia Malang
email: rofiq@asia.ac.id
[2] Ssitem Komputer, STMIK Asia Malang
email: bambangtriw@gmail.com

Abstract

Most of Safes lock system is still using conventional methods nowadays. The conventional method leads to the safes' burglary. Some of the causes are the safes' code that can be tracked easily and the key can be duplicated. Previous research on safes' security has ever been done. The weakness of the study is there is no security system using cryptographic algorithms for data security. The development of a safes security system by implementing ElGamal algorithms is done by following the engineering approach with the stages of methods analysis and design system, implementation and testing of the analysis and the discussion of the overall system. In the analysis and design of mathematical models using ElGamal algorithms, uses fast powering theorems and applications design uses Object Oriented Programming. In the analysis of hardware refers to the datasheet and calculation of the value of electrical characteristics of the circuit. In the safes lock system, the outcome of the research is a safes prototype which is equipped with enhancements that include a series of processing algorithms, the data viewer, a wireless data transfer device, the Android smartphone as a system of user authorization. For the lock safes systems is using a locked solenoid. The control system is done by a lock safes android smartphone via Bluetooth communication. The test results also indicate the system will open the safes if the code and the public key is entered correctly, and the system will not open if one of the codes or the public-keys are wrong or both are wrong.

Keywords: *ElGamal, Android, Atmega, Brankas*

1. PENDAHULUAN

a. Latar Belakang

Brankas merupakan suatu alat yang dipergunakan untuk menyimpan suatu barang atau aset-aset dan surat-surat yang berharga. (Erlina, 2013)

Beberapa faktor penyebab brankas bisa dibobol adalah pada umumnya, beberapa brankas masih menggunakan sistem rotari dan sistem penguncian menggunakan kunci manual.

Untuk pengendalian sistem lock brankas dapat digunakan mikrokontroler ATMEGA 16 dengan memberikan penyandian pada data kunci (password) brankas. Sistem penyandian ini dilakukan dengan teknik kriptografi menggunakan algoritma ElGamal. Dalam penyandian ini digunakan pula smartphone dan untuk komunikasi antara smartphone dengan mikrokontroler digunakan Bluetooth.

Berdasarkan pada beberapa kajian empiris tersebut maka penelitian ini akan mengimplementasikan algortima ElGamal pada sistem *lock* brankas melalui perangkat berbasis mikrokontroler ATMEGA16. Sedangkan *smartphone* android sebagai perangkat autentifikasi. Komunikasi mikrokontroler dengan *smartphone* melalui *bluetooth*.

b. *Rumusan Masalah*

Berdasarkan latar belakang di atas, maka perumusan masalah dalam penelitian ini adalah bagaimana mengimplementasikan algoritma *ElGamal* dalam sistem *lock* brankas berbasis mikrokontroler ATMEGA16 dan *smartphone* android.

c. Tujuan dan Manfaat

Berdasarkan perumusan masalah di atas maka tujuan penelitian ini adalah untuk meningkatkan tingkat keamanan sistem *lock* brankas dengan mengimplementasikan algoritma *ElGamal* yang berbasis mikrokontroler ATMEGA16 dan *smartphone* android. Adapun manfaat yang diharapkan dari penelitian ini adalah memberikan rasa aman lebih bagi pemilik

brankas dalam melindungi barang berharga dan bagi pihak kepolisian mampu menurunkan tingkat kriminalitas dalam kasus pembobolan brankas karena tingkat keamanan pada brankas yang semakin baik

d. Tinjauan Pustaka

Algoritma ElGamal

Algoritma ElGamal terdiri dari tiga proses, yaitu proses pembentukan kunci, proses enkripsi dan proses dekripsi. Algoritma ini merupakan cipher blok, yaitu melakukan proses enkripsi pada blok-blok plainteks dan menghasilkan blok-blok cipherteks yang kemudian dilakukan proses dekripsi, dan hasilnya digabungkan kembali menjadi pesan yang utuh dan dapat dimengerti. Untuk membentuk system kriptografi ElGamal, dibutuhkan bilangan prima p dan elemen primitif grup Z_p^*.

1) Pembentukan Kunci

Proses pertama adalah pembentukan kunci yang terdiri dari kunci rahasia dan kunci publik. Pada proses ini dibutuhkan sebuah bilangan prima *p* yang digunakan untuk membentuk grup Z_p^*, elemen primitif α dan sebarang $a \in \{0,1,..., p - 2\}$.

Kunci publik algoritma ElGamal berupa pasangan 3 bilangan, yaitu (p,α,β), dengan persamaan yang ditunjukkan dalam persamaan 2.7 (Schneier, 1996).

$$\beta = \alpha^a \bmod p \quad (1)$$

Sedangkan kunci rahasianya adalah bilangan *a* tersebut. Agar mempermudah dalam menentukan elemen primitif, digunakan bilangan prima *p* sedemikian hingga $p = 2.q+1$, dengan *q* adalah bilangan prima. Bilangan prima *p* seperti ini disebut dengan bilangan *prima aman*. Untuk menentukan apakah suatu bilangan itu prima atau komposit, dapat digunakan tes keprimaan seperti tes keprimaan biasa dan tes Miller-Rabbin. Karena digunakan bilangan bulat yang besar maka perhitungan pemangkatan modulo dilakukan penggunakan metode *fast exponentiation*. (Rinartha, 2010)

2) Enkripsi

Pada proses ini pesan dienkripsi menggunakan kunci publik (p,α,β) dan sebarang bilangan acak rahasia *k* $\in \{0,1,..., \pi - 2\}$. Misalkan *m* adalah pesan yang akan dikirim. Selanjutnya, *m* diubah ke dalam blok-blok karakter dan setiap karakter dikonversikan ke dalam kode ASCII, sehingga diperoleh plainteks $m_1, m_2, \ldots, m_n$ dengan $m_i \in \{1,2,\ldots,p-1\}\ dan\ i = 1,2,\ldots,n.$
Untuk nilai ASCII bilangan 0 digunakan untuk menandai akhir dari suatu teks.

Proses enkripsi pada algoritma ElGamal dilakukan dengan menghitung (Menezes, Oorschot and Vanstone, 1996)

$$\gamma = a^k \bmod p \quad (2)$$

dan

$$\delta = \beta^k . m \bmod p \ (3)$$

dengan *k* $\in \{0,1,..., p - 2\}$ acak. Diperoleh cipherteks (γ,δ).

Bilangan acak *k* ditentukan oleh pihak pengirim dan harus dirahasiakan, jadi hanya pengirim saja yang mengetahuinya, tetapi nilai *k* hanya digunakan saat melakukan enkripsi saja dan tidak perlu disimpan.

3) Dekripsi

Setelah menerima cipherteks (γ,δ) proses selanjutnya adalah mendekripsi cipherteks menggunakan kunci publik *p* dan kunci rahasia *a*. Dapat ditunjukkan bahwa plainteks *m* dapat diperoleh dari cipherteks menggunakan kunci rahasia *a*.

Diberikan (p,α,β) sebagai kunci publik dan *a* sebagai kunci rahasia pada algoritma ElGamal. Jika diberikan cipherteks (γ,δ), maka (Menezes, Oorschot and Vanstone, 1996)

$$m = \delta . (\gamma^a)^{-1} \bmod p \quad (1.4)$$

dengan *m* adalah plainteks. (Menezes, Oorschot and Vanstone, 1996)

Mikrokontroler ATMEGA 16

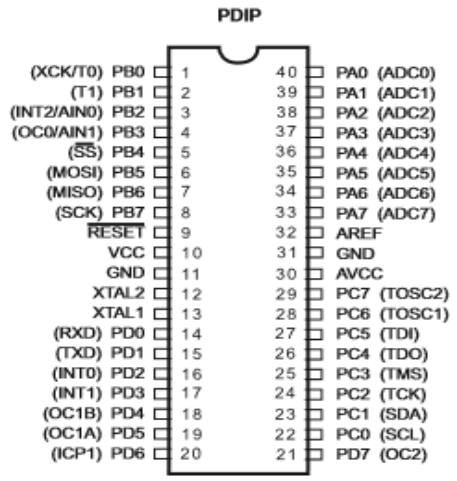
AVR merupakan seri mikrokontroler CMOS 8-bit buatan Atmel, berbasis arsitektur RISC (*Reduced Instruction Set Computer*). Fitur – fitur yang dimiliki mikrokontroler ATMEGA16 antara lain yaitu frekuensi clock maksimum 16 MHz, jalur I/O 32 buah, yang terbagi port A, port B, port C, dan port D (Putra, 2010)

Mikrokontroler ini menggunakan arsitektur Harvard yang memisahkan

memori program dari memori data, baik bus alamat maupun bus data, sehingga pengaksesan program dan data dapat dilakukan secara bersamaan (concurrent), adapun blog diagram arsitektur ATMEGA16.

Secara garis besar mikrokontroler ATMEGA16 terdiri dari :

1) Arsitektur RISC dengan throughput mencapai 16 MIPS pada frekuensi 16Mhz.
2) Memiliki kapasitas Flash memori 16 Kbyte, EEPROM 512 Byte, dan SRAM1Kb
3) Saluran I/O 32 buah, yaitu Port A, Port B, Port C, dan Port D.
4) CPU yang terdiri dari 32 buah register.
5) User interupsi internal dan eksternal
6) Port antarmuka SPI dan Port USART sebagai komunikasi serial
7) Fitur Peripheral
8) Dua buah 8-bit timer/counter dengan prescaler terpisah dan mode compare
9) Satu buah 16-bit timer/counter dengan prescaler terpisah, mode compare, dan mode capture
10) Real time counter dengan osilator tersendiri
11) Empat kanal PWM dan Antarmuka komparator analog
12) 8 kanal, 10 bit ADC
13) Byte-oriented Two-wire Serial Interface
14) Watchdog timer dengan osilator internal

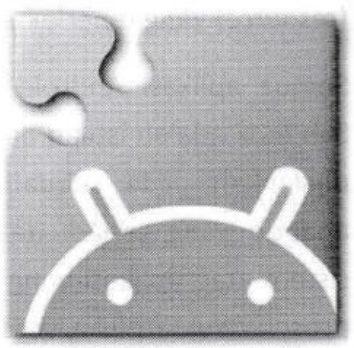


Gambar 1. Konfigurasi pin ATMEGA 16

Android

Android adalah sistem operasi yang berbasis Linux untuk telepon seluler seperti telepon pintar dan komputer tablet. Android menyediakan platform terbuka bagi para pengembang untuk menciptakan aplikasi mereka sendiri untuk digunakan oleh bermacam peranti bergerak. Android memiliki berbagai keunggulan sebagai piranti lunak yang memakai basis kode komputer yang bisa didistribusikan secara terbuka (open source) sehingga pengguna bisa membuat aplikasi baru di dalamnya.(Siregar, 2011)

App Inventor adalah sistem perangkat lunak untuk membuat aplikasi pada perangkat android. Uniknya, app inventor dibuat tidak seperti sistem pengembangan aplikasi biasa, dimana seorang programmer harus menuliskan baris-baris kode program, melainkan dengan interaksi visual berbasis grafis. Logo App Inventor ditunjukkan dalam Gambar 2.

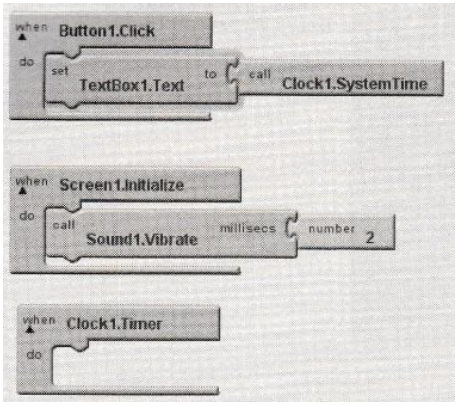


Gambar 2. Logo App Inventor

Interaksi programmer dengan App Inventor hampir sepenuhnya melalui antarmuka visual dengan operasi drag-and-drop. Secara sistem, app inventor terdiri dari dua komponen, yaitu *server* dan *client*. Server App Inventor berfungsi menyimpan semua asset program dan memberikan layanan lainnya terkait dengan manajemen berkas aplikasi (project). Sedangkan sisi client adalah aplikasi yang berhubungan langsung dengan programmer (pembuat aplikasi). (Mulyana, 2012)

Pada app inventor, salah satu fitur utamanya adalah memudahkan seseorang membuat program tanpa harus mengetikkan kode sedikitpun. Ini bisa diakomodasi menggunakan Bahasa block. Menggunakan Bahasa block, pengkodean dilakukan di belakang layar. Semuanya menggunakan antarmuka yang memudahkan bernama block/blok. Jadi blok ini merepresentasikan kode secara grafik. Cara Anda memasang block ini mirip dengan memasang puzzle

gambar, tapi sebenarnya cara memasang block ini akan sesuai dengan kode yang dihasilkan. (Wahana Komputer, 2013)



Gambar 3. Contoh kode-kode dari Puzzle

2. KAJIAN LITERATUR

Ivan C. Melalolin (2013) dalam penelitiannya yang berjudul "*Rancang Bangun Brankas Pengaman Otomatis Berbasis Mikrokontroler AT89S52"* menghasilkan sistem pengaman brankas otomatis yang menggunakan modem GSM selaku penghubung antara brankas dengan pemilik. . Setiap eksekusi pada brankas akan diberitahukan kepada pemilik melalui pesan singkat ke handphone pemilik. Nomor tujuan dapat diganti juga sesuai keinginan. Setiap karakter password dan nomor tujuan akan ditampilkan pada LCD. Brankas juga dilengkapi alarm serta LED indicator. Kendala yang didapat adalah brankas akan bekerja maksimal hanya pada area yang memiliki jangkauan sinyal GSM.

Perancangan pengaman brankas juga diteliti oleh Cresta Permana dan Tri Rahajoeningroem (2013) dalam penelitiannya yang berjudul "*Rancang Bangun Brankas Pengaman Otomatis Berbasis Multimedia Message Service (MMS) Menggunakan* ATMEGA*32"*. Penelitian ini merupakan pengembangan dari penelitan pengamanan brankas oleh Ivan C. Melalolin (2013). Dalam pengembangan ini, brankas ditambahkan fasilitas *image* kamera yang berguna untuk me*monitoring* keadaan brankas serta adanya penambahan fasilitas untuk mengetahui jumlah pulsa dan masa aktif *SIMCard* yang terdapat pada GSM. GSM *Module* digunakan sebagai media penghubung untuk pengiriman pesan singkat (SMS) dan pesan multimedia (MMS) kepada pemilik yang berfungsi memberikan informasi keadaan brankas.

Pengembangan pengamanan brankas juga diteliti oleh Risa dkk pada tahun 2013 mendesain *prototype* brankas yang mudah dipantau dari jarak jauh oleh pemiliknya. Sistem pengaman brankas ini berhasil dibangun dengan prinsip kerja kunci pengaman brankas ini dapat dibuka dengan memasukkan kode *password* yang benar dan apabila kode *password* yang dimasukkan salah maka sistem akan membunyikan *alarm buzzer* serta mengirim SMS peringatan ke nomor pemilik brankas yang telah diprogram pada mikropengendali. Pengembangan pengamanan brankas yang serupa juga pernah diteliti oleh Erlina dan Bambang (2013).

Pada penelitian yang lain Afrida (2014) mengembangkan sistem pengamanan brankas dengan *voice smartphone* dalam penelitiannya yang berjudul "*Pengaman Brankas Menggunakan Voice Smartphone Pada SDN Kedaung Wetan 8 Dengan Media Bluetooth Berbasis Mikrokontroller* ATMEGA *328*". Dalam penelitian ini dimanfaatkan *bluetooth* dalam media komunikasinya.

3. METODE PENELITIAN

Jenis Penelitian

Penelitian ini termasuk penelitian rekayasa aplikasi, yaitu suatu kegiatan merancang (design) yang tidak rutin, sehingga di dalamnya terdapat kontribusi baru, baik dalam bentuk, proses maupun produk.

Jenis dan Sumber Data

Jenis data yang digunakan dalam penelitian ini adalah data kuantitatif (angka/bilangan) yang berupa angka yang akan disandikan. Sedangkan sumber data diperoleh dari tipe angka pada *Operating System* Android dan mikrokontroler.

Tahapan-Tahapan Penelitian

Tahapan secara keseluruhan yang dilakukan dalam menyelesaikan penelitian ini adalah sebagai berikut:

1. Pra Penelitian:
   Kegiatan pada pra penelitian adalah kegiatan awal untuk menentukan bahan yang akan digunakan, menentukan teori penunjang, menentukan jurnal yang terkait dan menentukan perangkat lunak pendukung yang akan digunakan untuk simulasi serta pendalaman penggunaannya.

2. Identifikasi masalah
   Identifikasi masalah yang menjadi dasar permasalahan yang akan dijawab dalam penelitian ini.
3. Penetapan tujuan
   Pernyataan secara konkrit dan jelas tentang apa yang ingin dicapai dari solusi masalah yang telah dirumuskan dan dikaji sesuai sudut pandang.
4. Analisis teori
   Menganalisis teori yang mendukung penelitian ini yang meliputi jenis data dan cara mendapatkan data, analisis data, variabel dalam algoritma yang digunakan.
5. Perancangan program aplikasi
   Untuk mengaplikasikan dari teori dan algoritma yang digunakan maka dibutuhkan program aplikasi.
6. Implementasi program aplikasi
   Implementasi dari rancangan aplikasi yang telah dibuat dalam program aplikasi.
7. Pengujian program
   Pengujian program sebagai sarana pengujian apakah rancangan yang telah dilakukan sesuai dengan analisis teori.
8. Kesimpulan dan Saran
   Kesimpulan dibuat berdasar hasil analisis dan tujuan penelitian. Saran dibuat berdasarkan kelemahan sistem dengan tujuan untuk perbaikan.

Lokasi Penelitian

Penelitian ini dilaksanakan di Laboratorium Otomasi dan Elektronika Program Studi Sistem Komputer STMIK Asia Malang.

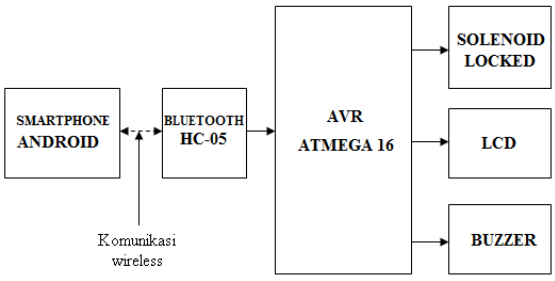
Hipotesis

Hipotesis dari penelitian yang dibuat adalah algoritma ElGamal dapat digunakan untuk enkripsi maupun dekripsi sistem *lock* brankas.

4. HASIL DAN PEMBAHASAN

Perancangan dan Implementasi

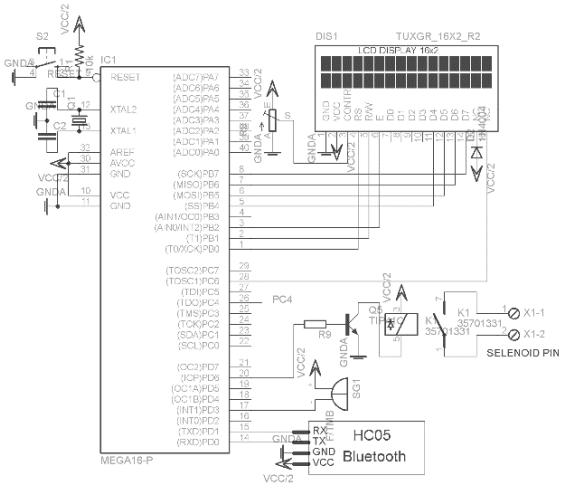
Blok diagram sistem ditunjukkan dalam Gambar 4.



Gambar 4. Blok Diagram Perancangan

Dari blok diagram perancangan pada Gambar 4., *smartphone* dan mikrokontroler sebagai perangkat yang melakukan proses penyandian. Sedangkan buzzer sebagai peringatan adanya suatu kesalahan dalam proses. Untuk solenoid *locked* itu sebagai sistem buka tutup dari pintu brankas. LCD berfungsi sebagai penampil kunci publik serta status dari masing-masing proses yang dikerjakan. Bluetooth sebagai komunikasi antara mikrokontroler (brankas) dengan smartphone.

Untuk rangkaian keseluruhan sistem ditunjukkan dalam Gambar 5.

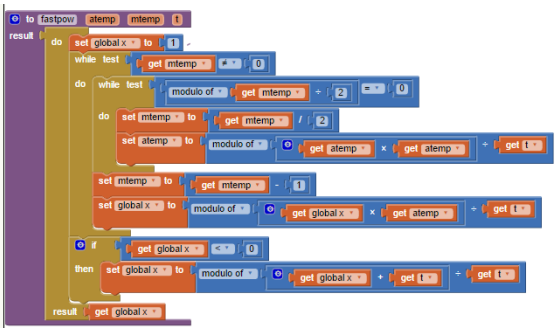


Gambar 5. Rangkaian Keseluruhan Perangkat Keras pada Brankas

Untuk implementasi algoritma ElGamal dilakukan dengan tiga tahap yaitu pembentukan kunci publik, enkrpsi dan dekripsi. Dalam perhitungan matematisnya digunakan fungsi *fast powering*. Listing program fungsi fast powering pada ATMEGA ditunjukkan dalam Gambar 6 dan pada Android ditunjukkan dalam Gambar 7.

```
int fastpow(long int r,long int s,long int t)
{
 long int atemp=r,mtemp=s,x=1;
 while(mtemp!=0)
 {
  while((mtemp%2)==0)
  {
   mtemp=mtemp/2;
   atemp=(atemp*atemp)%t;
  }
  mtemp=mtemp-1; x=(x*atemp)%t;
 }
 if(x<0) x=(x+t)%t;
 return x;
}
```

Gambar 6. Listing Program Fungsi Fast Powering pada ATMEGA



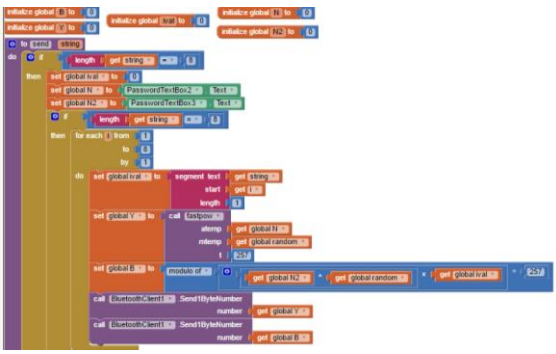
Gambar 7. Fungsi Fast Powering pada Android

Untuk pembentukan kunci publik diimplementasikan listing program dalam Gambar 8.

```
char create_key(long int g,long int x)
{
 long int y;
 long int p=257;
 y=fastpow(g,x,p);
 return y;
}
```

Gambar 8. Listing Program Kunci Publik

Selanjutnya Listing program untuk enkripsi ditunjukkan dalalm Gambar 9.



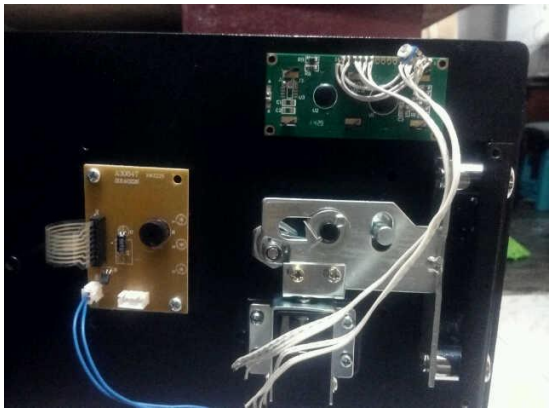
Gambar 9. Listing Program Enkripsi

Untuk listing program dekripsi ditunjukkan dalam Gambar 10.

```
char dekrip(long int y,long int b,long int x)
{
 long int m;
 m=fastpow(y,x,257);
 m=(fastpow(m,257-2,257)*b)%257;
 return m;
}
```

Gambar 10. Listing Program Dekripsi

Untuk tampilan perangkat keras pada brankas Gambar 11.



Gambar 11. Perangkat Keras pada Brankas

Sedangkan untuk tampilan antarmuka pengguna pada smartphone android ditunjukkan dalam Gambar 12.

Gambar 12. Antarmuka Pengguna pada Android

Pengujian

1) Pengujian pembentukan kunci publik

Proses pembentukan kunci publik dilakukan pada program di brankas. Pada pembentukan kunci publik ini, nilai kunci private yang digunakan yaitu 13 dengan bilangan prima bernilai 257. Hasil pengujian program pembentukan kunci publik baik output program maupun perhitungan manual ditunjukkan dalam Tabel 1.

Tabel 1. Hasil Pengujian Pembentukan Kunci Publik

No	Kunci Acak	Kunci Publik	
		Program	Manual
1	37	107	107
2	22	67	67
3	49	195	195
4	99	199	199
5	50	215	215
6	44	169	169
7	24	181	181
8	67	123	123
9	20	147	147
10	1	1	1
11	89	143	143
12	76	45	45
13	53	14	14
14	3	152	152
15	13	36	36
16	75	71	71
17	71	217	217
18	97	202	202

Dari hasil pengujian yang ditunjukkan dalam Tabel 1. menunjukkan bahwa output program sesuai hasil perhitungan pada persamaan 1. Dengan demikian kunci publik yang dihasilkan oleh program bernilai benar dalam perhitungannya

a. Pengujian Proses Enkripsi

Perhitungan enkripsi dilakukan oleh smartphone android. Pada proses enkripsi ini kunci publik yang digunakan berdasarkan kunci publik yang dihasil oleh sistem pada brankas. Hasil proses enkripsi oleh smartphone akan dikirim ke sistem pada brankas untuk ditampilkan di LCD via Bluetooth. Untuk pengujian awal digunakan plaintext berupa kode (pesan) bernilai 1234 dengan kunci publik 103. Untuk kunci tambahan dan bilangan acak dirandom oleh sistem.

Dalam proses enkripsi ini, plaintext yang dienkripsi akan menghasilkan chipertext 1 dan chipertext 2. Hasil data pengujian yang ditunjukkan dalam Tabel 2.

Tabel 2. Hasil Pengujian Proses Enkripsi

Plaintext (kode/pesan)	Chipertext 1	Chipertext 2
1	217	78
2	217	156
3	217	234
4	217	55

Hasil perhitungan enkripsi pada program selanjutnya akan diuji dengan perhitungan manual sesuai dengan persamaan 2 dan 3. Untuk kunci tambahan dan nilai acak random yang dihasilkan sistem bernilai 38 dan 67.

Hasil perhitungan proses enkripsi adalah sebagi berikut :

Diketahui: (kunci tambahan=38; nilai acak=67; kunci publik=103; bil prima=257; plaintext=1)

$$\gamma = a^k \bmod p$$
$$= 38^{67} \bmod 257$$
$$= 217$$

$$\delta = \beta^k . m \bmod p$$
$$= 103^{67} . 1 \bmod 257$$
$$= 78$$

Dari hasil perhitungan manual ini maka nilai perhitungan program telah sesuai dengan persamaan yang digunakan. Dengan perhitungan yang sama hasil chipertext 1 dan 2 dari plaintext data berikutnya yaitu 2,3,4 juga menghasilkan hasil perhitungan yang sesuai.

b. Pengujian proses dekripsi

Perhitungan dekripsi dilakukan oleh brankas. Pada proses dekripsi ini kunci private yang digunakan bernilai 13. Hasil perhitungan proses dekripsi akan ditampilkan di LCD. Untuk chipertext yang digunakan berdasarkan data yang ditunjukkan dalam Tabel 2. Hasil pengujian proses dekripsi ditunjukkan dalam Gambar 13.

Gambar 13. Hasil pengujian dekripsi

Berdasarkan hasil pengujian yang ditunjukkan dalam Gambar 4.10 menunjukkan bahwa proses dekripsi telah sesuai dengan penghitungan.

2) Pengujian Plaintext dengan Hasil Dekripsi

Pada pengujian ini untuk menguji apakah sistem mampu membaca kode atau pesan yang dikirim. Hasil pengujian perbandingan plaintext dengan hasil dekripsi ditunjukkan dalam Tabel 4.3.

Tabel 3. Hasil Pengujian Perbandingan Plaintext dengan Hasil Dekripsi

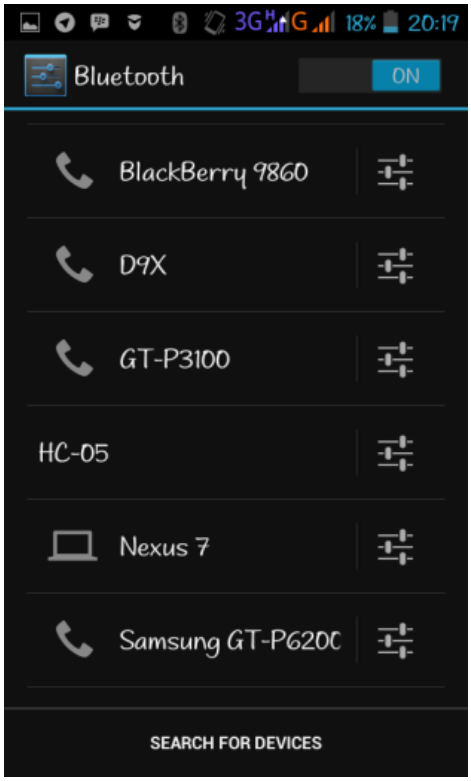
Kode (plaintext)	Kunci Publik	Hasil enkripsi		Hasil dekripsi
		Chipertext 1	Chipertext 2	
27895432	107	236,236,236,236, 236,236,236,236	199, 54, 25, 253, 112,141,170,199	27895432
71429062	67	30,30,30,30, 30,30,30,30	188,137,34,17, 205,0,51,17	71429062
23527689	195	123,123,123,123, 123,123,123,123	162,243,148,162, 53,229,134,215	23527689
78674162	199	211,211,211,211, 211,211,211,211	251,140,105,251, 70,146,105,35	78674162
66590571	215	92,92,92,92, 92,92,92,92	19,19,230,157, 0,230,65,46	66590571
98761234	169	120,120,120,120, 120,120,120,120	208,242,19,53, 223,189,155,121	98761234
75312468	181	217,217,217,217, 217,217,217,217	32,133,234,78, 156,55,211,110	75312468
23977980	123	165,165,165,165, 165,165,165,165	165,119,100,192, 192,100,146,0	23977980
39568799	147	127,127,127,127, 127,127,127,127	207,107,88,157, 38,226,107,107	39568799
45162387	1	1,1,1,1,1,1,1,1	4,5,1,6,2,3,8,7	45162387
65870942	143	49,49,49,49, 49,49,49,49	142,204,18,80, 0,213,9,133	65870942
35759842	45	179,179,179,179, 179,179,179,179,	4,178,95,178, 12,182,91,174	35759842
79816532	14	166,166,166,166, 166,166,166,166	121,229,175,54, 67,13,163,108	79816532
91834567	152	63,63,63,63, 63,63,63,63,	94,39,55,117, 156,195,234,16	91834567
98765432	36	215,215,215,215, 215,215,215,215,	128,228,71,171, 14,114,214,57	98765432
51496487	71	212,212,212,212, 212,212,212,212	234,201,33,10, 178,33,66,122	51496487
31479826	217	201,201,201,201, 201,201,201,201	62,192,254,59, 186,251,127,124	31479826
59813476	202	48,48,48,48, 48,48,48,48	81,43,181,119, 100,219,62,200	59813476
76532489	35	190,190,190,190, 190,190,190,190	167,33,156,145, 11,22,44,178	76532489
42753896	56	164,164,164,164, 164,164,164,164,	5,131,73,199, 68,10,204,136	42753896

Dari data hasil pengujian yang ditunjukkan dalam Tabel 3 menunjukkan bahwa sistem mampu melakukan proses enkripsi dan dekripsi dengan benar.

3) Pengujian Keseluruhan Sistem

Sedangkan untuk pengujian sistem dilakukan dengan menginputkan beberapa kode yang berbeda dengan nilai yang benar dan nilai yang salah untuk mengetahui sistem berjalan sesuai yang diharapkan. Langkah-langkah pengujiannya yaitu :

a. Koneksikan bluetooth pada smartphone dengan brankas. Nama Bluetooth di brankas yaitu HC-05. Tampilan bluetooth HC-05 pada smartphone ditunjukkan dalam Gambar 14.



Gambar 14. Tampilan bluetooth HC-05 pada smartphone

b. Cek nilai password (kunci publik) dengan melihat nilai di LCD yang dihasilkan oleh sistem pada brankas. Nilai password ditunjukkan dalam Gambar 15.

Gambar 15. Nilai password

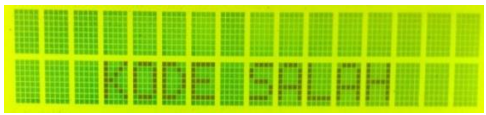
c. Input kode dan password yang sudah ada. Setelah diinputkan selanjutnya tekan tombol kirim. Input kode dan password ditunjukkan dalam Gambar 16.

Gambar 16. Input kode dan password

d. Jika kode benar maka brankas terbuka dan ditampilkan status dari brankas tersebut. Serta peringatan supaya setelah selesai menggunakan brankas agar menekan tombol agar brankas terkunci kembali. Jika hasil kode salah maka muncul peringatan kode salah. Hasil kode yang benar ditunjukkan Gambar 17 dan Gambar 18. Sedangkan jika kode salah ditunjukkann dalam Gambar 19.

Gambar 17. Tampilan kondisi brankas jika hasil kode benar

Gambar 18. Tampilan selama brankas terbuka



Gambar 19. Tampilan kondisi brankas jika kode salah

Hasil pengujian sistem keseluruhan ditunjukkan dalam Tabel 4.

Tabel 4. Hasil pengujian sistem keseluruhan

Kunci Publik	Kunci publik yang dimasukkan	Kode sistem	Kode yang dimasukkan	Output sistem	Keterangan
108	108	57690234	57690234	Brankas terbuka	Kunci publik dan kode sesuai
304	215	56893561	56893561	Brankas tertutup (kode salah)	Kunci publik tidak sesuai, kode sesuai
202	202	98567234	98567268	Brankas tertutup (kode salah)	Kunci publik sesuai, kode tidak sesuai
35	69	1235678	7689354	Brankas tertutup (kode salah)	Kunci publik dan kode tidak sesuai

Dari hasil pengujian yang ditunjukkan dalam Tabel 4. maka dapat dianalisis sebagai berikut:

a. Brankas akan terbuka jika kunci publik dan kode yang dimasukkan sesuai
b. Brankas tetap tertutup jika salah satu dari kunci publik atau kode salah dan juga jika kedua-duanya salah

5. KESIMPULAN

Dari hasil penelitian dan pembahasan yang telah diuraikan dalam bab sebelumnya, maka dapat dibuat kesimpulan sebagai berikut.

a. Pengembangan sistem pengamanan brankas dengan mengimplementasikan algoritma ElGamal pada sistem *lock* brankas berbasis mikrokontroler ATMmega16 dan *smartphone* android via *bluetooth* dilakukan mengikuti pendekatan engineering dengan tahapan-tahapan metode analisis dan disain sistem, implementasi dan analisis pengujian serta pembahasan sistem secara keseluruhan.
b. Dalam analisis dan disain model matematis algoritma ElGalam digunakan teorema *fast powering*.
c. Untuk kode yang dimasukkan sebanyak 8 digit yang dalam prosesnya kode tersebut disandikan per digit.
d. Dari hasil pengujian juga menunjukkan sistem akan membuka brankas jika kode dan kunci publik yang dimasukkan benar, dan sistem tidak akan terbuka jika salah satu dari kode atau kunci publik bernilai salah atau kedua-duanya bernilai salah.

6. REFERENSI

[1] Erlina, C, dan Purnama, B, 2013. Sistem Pengaman Brankas Dengan Menggunakan Handphone Berbasis Mikrokontroler AT89S51, Seruni, Vol 2, No 1, pp 1-7

[2] Melalolin, I, 2013, Rancang Bangun Brankas Pengaman Otomatis Berbasis Mikrokontroler AT89S52, Jurnal Telekontran, Vol 1, No 1, pp 59-66

[3] Menezes, A. J. Oorschot, P.C.v. Vanstone, S. A. 1997. Handbook of Applied Cryptography, CRC Press ISBN 0-8493-8523-7.

[4] Mulyana, E. 2012. App Inventor: Ciptakan Sendiri Aplikasi Androidmu, Yogyakarta, Andi

[5] Permana, C and Rahajoeningroem, T, Oktober 2013, Rancang Bangun Brankas Pengaman Otomatis Berbasis Multimedia Message Service (MMS) Menggunakan ATMEGA32, Jurnal Telekontran, Vol 1, No 2, pp 27-37

[6] Putra, A, 2010, Tips dan Trik Mikrokontroler AT89 dan AVR, Yogyakarta, Gava Media

[7] Rinartha, K, 2010, Pengamanan Citra Digital Dengan Menggunakan Pengembangan Kriptografi Kunci Public Elgamal, Prosiding Seminar Nasional Teknologi Informasi dan Aplikasinya Volume 2, Politeknik Negeri Malang

[8] Risa, dkk. 2013. Purwarupa Sistem Pengaman Brankas Menggunakan Keypad Dan Handphone, Tugas Akhir Prodi D3 Teknik Telekomunikasi STT Telematika Telkom, Purwokerto

[9] Siregar, I, 2011, Membongkar Source Code berbagai Aplikasi Android, Yogyakarta, Gava Media

[10] Wahana Komputer, 2013, Membuat Apliaksi Android Tanpa Coding dengan App Inventor, Jakarta, Elex Media Komputindo

[11] Yuswanto, A, 2014. Pengaman Brankas Menggunakan Voice Smartphone Pada SDN Kedaung Wetan 8 Dengan Media Bluetooth Berbasis Mikrokontroller ATMEGA 328, Tugas Akhir Jurusan Sistem Komputer STMIK Raharja, Tangerang